In the Specification:

Please replace the current paragraph [0026] with the below listed paragraph [0026]

[0026] Referring to FIG. 1, the initial process of the invention is to establish a list of protected symbolic links in the security policy database. In this process, the native operating system scans each file for which external security protection is desired. For each scanned file, there has to be a determination of whether that file is a symbolic link file. For each scanned file, the first step 10 is to get the attributes of that file. The file attributes contain information about the file. One piece of information contain in the file attributes is whether the file is a symbolic link. Step 11 makes the determination of whether the file is a symbolic link. Since the methods of the present invention relate only to protection of symbolic link files, if the file is not a symbolic link, the methods of the present invention will not apply. In this case, the method moves to step 12 where this method would end with the normal processing of adding file resource as a protected resource in the database of protected resources. If step 11 determines that this file is a symbolic link, step 13 will retrieve the name of the target file pointed to by this symbolic link. Since the present file to be protected is a symbolic link, there is a desire to protect the underlying target file pointed to by this symbolic link. The symbolic link only contains the name of the target file, there is no independent reason to protect a symbolic link file apart from the underlying target file. Therefore, step 14 adds the symbolic link and target resource to the security database as protected resources. The target file will have the same security rules and protections applied to it that are applied to the symbolic link that points to this target file. The details of step 14 are further described in FIG. 2.

Please replace the current paragraph [0026] with the below listed paragraph [0028]

[0028] FIG. 3 illustrates the steps involved in the technique of the present invention to implement the external security policy rules on system access attempts through symbolic links. An example of a security policy rule is a restriction on when a certain or group can access a system resource. In this method, during a system access attempt, the file object information for the accessed resource is retrieved. The retrieved information will reveal that this file is a symbolic link, which points to a target resource. Step 20 locates the resource named in the symbolic link. After retrieving the object information for this target resource, the next step 21 is to search the protected database created in FIG. 1 for that target resource. If a search did not find the resource in the database step 22, this would mean that the target resource is not protected by the external security policy. Since there is no protection on this target resource, this method does not have relevance to the system security. In this instance, the method would terminate in step 23. If the search resulted is a found target resource/object, step 22, then this search result means that security policy does protect this resource.

In the Drawings;

Please replace the current Figure 6 with the enclosed Figure 6.